

UNITED STATES DISTRICT COURT

for the
Middle District of North Carolina

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*Facebook Accounts With User ID 100001272827882
And 100018319993329

Case No. 1:18mj305

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

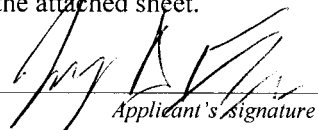
- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 USC § 2251(a)	Production of Child Pornography
18 USC § 2252A(a)(2)(A)	Distribution/Receipt of Child Pornography
18 USC § 2252A(a)(5)(B)	Possession of Child Pornography

The application is based on these facts:

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Jerry D. Faulk, FBI Task Force Officer
Printed name and title

Sworn to before me and signed in my presence.

Date: 10/03/18

*Judge's signature*City and state: Greensboro, North Carolina

L. Patrick Auld, United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Jerry D. Faulk, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with the Facebook user ID numbers 100001272827882 and 100018319993329 that is stored at premises owned, maintained, controlled, or operated by Facebook, Inc. ("Facebook"), a company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Facebook, Inc. to disclose to the government records and other information in its possession pertaining to the subscriber or customer with the user ID numbers.

2. I, Jerry D. Faulk, am a Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI) in the Charlotte Division. I am currently assigned to the Child Exploitation Task Force (CETF). I was sworn in as a Special Deputy U.S. Marshal assigned to the FBI in April 2018. In December 1997, I graduated from East Carolina University with a Bachelor of Science Degree in Criminal Justice. I was hired by the Raleigh Police Department in June 1999 and graduated from the police academy in December 1999. I became a detective

in November 2004 and have been assigned to General Investigations, the Robbery Unit, and the Homicide Unit. I became a member of the North Carolina Internet Crimes against Children (NCICAC) Task Force in December 2017. In my career, I have participated in several investigations involving the production, distribution, and possession of child pornography. I have also received training in the area of child pornography and child exploitation, and have observed numerous examples of child pornography as defined in 18 U.S.C. § 2256. As a TFO assigned to the FBI, I am authorized to investigate violations of federal laws and request and execute search warrants issued under the authority of the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, and information provided to me by other law enforcement agents, Facebook, Inc., and the National Center for Missing and Exploited Children (NCMEC). This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. I am investigating a case involving multiple child exploitation offenses including violations of 18 U.S.C. §§ 2251(a), 2252A(a)(2)(A), and 2252A(a)(5)(B). Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to search the information described in

Attachment A for contraband and evidence, fruits, and instrumentalities of these violations, more particularly described in Attachment B.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations relating to the sexual exploitation of minors.

a. 18 U.S.C. § 2251(a) prohibits a person from, using, persuading, inducing, enticing, or coercing any minor to engage in, or having a minor assist any other person to engage in, or transporting any minor in or affecting interstate or foreign commerce, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce. As

described in 18 U.S.C. § 2251(e), attempts and conspiracies to violate 18 U.S.C. § 2251 fall under that section.

b. 18 U.S.C. § 2252A(a)(2)(A) prohibits a person from knowingly receiving, distributing or conspiring to receive or distribute any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

c. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

PROBABLE CAUSE

6. In June 2017, the National Center for Missing and Exploited Children (NCMEC) received information from Facebook, Inc. regarding the distribution and receipt of child exploitation images on the Facebook social media platform. Facebook, Inc. reported that the user of the Facebook account ID 100001272827882 (Subject Account-1) was enticing two minor Facebook users, both reportedly born in 2003, to produce and send child exploitation images. According to Facebook, Inc., Subject Account-1 has a username of alex.aguilar.16906 and lists a date of birth of 1992. The minors will be referred to as C.G. and E.C.

7. In NCMEC CyberTipline Report 21542800, Facebook, Inc. reported that minor C.G. sent Subject Account-1 fifty-three images depicting the genital and anal areas of a minor male subject. Facebook, Inc. reported the incident date as May 25, 2017. Two of the images are as follows:

“1vi3o4pba97o044c18718406_436595543368354_916604833_n.jpg” is a still image that depicts the erect penis of a male subject approximately 12-13 years old.

“bv1ry090qtc0ogos19014468_442055396155702_2481466292121370624_n.mp4” is a video file that depicts a male subject approximately 12-13 years inserting his finger into his anus.

8. In NCMEC CyberTipline Report 21542815, Facebook, Inc. reported that minor E.C. sent Subject Account-1 five images depicting the genital and anal areas of a male subject approximately 12-13 years old. Facebook, Inc. reported the incident date as May 25, 2017. Two of the images are as follows:

“30lg4vvsqk004k4c18716710_226563757839241_2114881301_n.jpg” is a still image that depicts the penis of a male subject approximately 12-13 years old.

“9nn85lsbdickkk4c18706087_226565547839062_86545510864781312_n.mp4” is a video file that depicts a male subject approximately 12-13 years old inserting his finger into his anus.

9. In NCMEC CyberTipline Report 21542777, Facebook, Inc. reported that Subject Account-1 uploaded an image on May 28, 2017 and then another image on May 29, 2017. The images are as follows:

“evql2ucrzm04ckwo18741676_437247943303114_85614390_n.jpg” is a still image that depicts a male subject approximately 12-13 years old with his genital and anal areas exposed.

“ca8ysq23i7swocs818788712_437973386563903_2070588353_n.jpg” is a still image that depicts the anus of a male subject approximately 12-13 years old.

Facebook, Inc. reported that both of these images were uploaded using IP address 71.69.193.186.

10. In NCMEC CyberTipline Report 22575646, Facebook, Inc. reported that Subject Account-1 enticed minors C.G. and E.C. to produce and send child exploitation images. In the report to NCMEC, Facebook, Inc. included excerpts from sexually explicit communications¹ between Subject Account-1 and the minors. The chats between Subject Account-1 and C.G. are dated from May 12, 2017 to June 7, 2017. The chats between Subject Account-1 and E.C. are dated from May 18, 2017 to May 26, 2017. The chats include the following:

C.G. & Subject Account-1:

May 25, 2017:

Subject Account-1	Do you have school
<i>C.G.</i>	<i>Yes from</i>
<i>C.G.</i>	<i>From 1 to 5</i>
Subject Account-1	What grade are you in?
<i>C.G.</i>	<i>7 seventh</i>
Subject Account-1	That's great
Subject Account-1	Are you 14 years old
Subject Account-1	??
<i>C.G.</i>	<i>I'm 13</i>

May 26, 2017:

<i>C.G.</i>	<i>I sent you plenty</i>
Subject Account-1	haha
<i>C.G.</i>	<i>And naked</i>
Subject Account-1	delete them

May 30, 2017:

Subject Account-1	I want a video where you masturbate your little butt but I know you wouldn't dare
<i>C.G.</i>	<i>Fine but later</i>
Subject Account-1	Mmm
<i>C.G.</i>	<i>And how do I masturbate my behind?</i>

¹ In the NCMEC report the communications are listed in Spanish and appear to have been translated into English by Facebook, Inc.

E.C. & Subject Account-1:

May 18, 2017:

Subject Account-1	And how old are you
<i>E.C.</i>	<i>Guess</i>
<i>E.C.</i>	<i>Are</i>
<i>E.C.</i>	<i>Old</i>
<i>E.C.</i>	<i>You</i>
<i>E.C.</i>	<i>How</i>
<i>E.C.</i>	<i>old are you</i>
Subject Account-1	24
<i>E.C.</i>	<i>12 years old</i>
Subject Account-1	God
Subject Account-1	You are a kid
Subject Account-1	Heheh

May 26, 2017:

Subject Account-1	I want to see it sticking up
<i>E.C.</i>	<i>And from outside</i>
Subject Account-1	?
<i>E.C.</i>	[image reported by Facebook, Inc. as a child exploitation image]
Subject Account-1	It's up
<i>E.C.</i>	[image reported by Facebook, Inc. as a child exploitation image]
<i>E.C.</i>	<i>Yes</i>
<i>E.C.</i>	<i>I want to see yours</i>
Subject Account-1	Open up your little butt baby
Subject Account-1	I want to see it good
<i>E.C.</i>	<i>Oh god</i>
Subject Account-1	What
<i>E.C.</i>	<i>Now it's your turn</i>
<i>E.C.</i>	<i>You</i>
<i>E.C.</i>	<i>I already sent to you</i>

11. NCMEC CyberTipline Report 22575646 also documents that the user of Facebook account ID 100018319993329 (Subject Account-2)

communicated² on Facebook with C.G. on June 22 and 23, 2017. Facebook, Inc. reported that Subject Account-1 is linked by machine cookies to Subject Account-2. An excerpt follows:

C.G. & Subject Account-2:

June 22, 2017:

C.G.	[image reported by Facebook, Inc. in CyberTipline Report 22513931 depicting the anal area of a male subject approximately 12-14 years old]
Subject Account-1	Mmmm

12. Facebook, Inc. reported that Subject Account-1 was accessed from IP address 71.69.193.186 on May 13, 2017, June 11, 2017, and July 18, 2017. Records for the IP address were subpoenaed on July 20, 2017 and resolve to 1822 Stage Road, Durham, NC 27703. IP address 71.69.193.186 was leased to this account from, at least, October 30, 2016 to June 27, 2017.

13. A preservation order was sent to Facebook, Inc. on June 21, 2018 requesting the records for Subject Account-1 and Subject Account-2 be retained. As of October 2, 2018, the accounts were not active when searched on Facebook. In my experience, even when a particular account has been removed from Facebook, Facebook, Inc. may still have information regarding the account.

FACEBOOK

² In the NCMEC report the communications are listed in Spanish and some appear to have been translated into English by Facebook, Inc.

14. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

15. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

16. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News

Feed,” which highlights information about the user’s “Friends,” such as profile changes, upcoming events, and birthdays.

17. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create “lists” of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

18. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. In addition, Facebook users can “check in” to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or her “Friends” can

post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

19. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

20. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

21. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

22. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.

23. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

24. Each Facebook account has an activity log, which is a list of the user’s posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

25. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs (“blogs”), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

26. The Facebook Gifts feature allows users to send virtual “gifts” to their friends that appear as icons on the recipient’s profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other “pokes,” which are free and simply result in a notification to the recipient that he or she has been “poked” by the sender.

27. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.

28. Facebook uses the term “Neoprint” to describe an expanded view of a given user profile. The “Neoprint” for a given user can include the following information from the user’s profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification numbers; future and past

event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications.

29. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

30. Facebook also retains User Agent strings associated with each transaction associated with an IP address. The User Agent is information transmitted by the device being used to browse a web page that identifies the type of device and type of web browser being used. Websites use this information to adjust the way the content is displayed for the device for compatibility and readability purposes.

31. Cookies are small pieces of text used to store information on web browsers. Cookies store and receive identifiers and other information on computers, phones and other devices. Facebook uses cookies for several reasons including security and authentication purposes. When a Facebook user logs into their account, a “machine cookie” is set for the particular device being used.

Machine cookies can be used to determine if different Facebook accounts are logged into from the same device.

32. As of June 2013, Facebook serviced over 1.15 billion active users and more than 819 million use Facebook on a mobile device on a daily basis. Facebook can be accessed via the internet by visiting <http://www.facebook.com> or via the free Facebook application that is available for most mobile devices using the Apple iOS mobile operating system (used by Apple iPhones, iPads, and iPod Touch devices) or the Google Android mobile operating system (used by Android phones and tablet devices). Facebook data is stored on servers controlled by Facebook and may not be stored directly on a user's computer or mobile device though computer forensic evidence may be present on the device indicating Facebook use.

33. Facebook users can enable specific mobile telephones to access their accounts by logging into their Facebook account and designating the mobile device telephone number to be authorized. Enabling a mobile device allows Facebook to send SMS text message notifications for friend requests, messages, Wall posts, and status updates from friends. Users can also update their status, search for phone numbers, or upload photos and videos from a phone. In order to enable this feature, the user must enter the device telephone number, and receive a confirmation code from Facebook; this code must then be entered

via the Facebook account portal on the primary Facebook website for the device to be authorized.

34. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

35. Information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. in my training and experience, a Facebook user's "Neoprint," IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while

executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Facebook “friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner’s state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a

plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

36. Therefore, the account servers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

37. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

38. Because the warrant will be served on Facebook, Inc., who will then compile the requested records at a time convenient to Facebook, Inc., reasonable cause exists to support execution of the requested warrant at any time day or night.

CONCLUSION

39. Based on the forgoing, I request that the Court issue the proposed search warrant.

40. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States ... that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

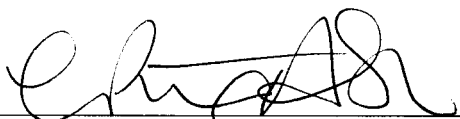
41. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,



Jerry D. Faulk
Task Force Officer
Federal Bureau of Investigation

Subscribed and sworn to before me on 10/03, 2018.



L. Patrick Auld
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Facebook user ID numbers 100001272827882 and 100018319993329 from April 1, 2017 to October 3, 2018 which is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in Menlo Park, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook Inc. ("Facebook"), including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A for the period of April 1, 2017 to October 3, 2018:

- (a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;
- (b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;
- (c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos ;
- (d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future

and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications;

- (e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, the user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;
- (f) The identity of other accounts linked by machine cookie and the nature of the cookie;
- (g) All other records of communications and messages made or received by the user, including all Messenger activity, private messages, chat history, video and voice calling history, and pending “Friend” requests;
- (h) All “check ins” and other location information;
- (i) All IP logs, including all records of the IP addresses that logged into the account and their user agent strings;
- (j) All records of the account’s usage of the “Like” feature, including all Facebook posts and all non-Facebook webpages and content that the user has “liked”;
- (k) All information about the Facebook pages that the account is or was a “fan” of;
- (l) All past and present lists of friends created by the account;
- (m) All records of Facebook searches performed by the account;
- (n) All information about the user’s access and use of Facebook Marketplace;
- (o) The types of service utilized by the user;

- (p) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (q) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
- (r) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

Facebook is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes contraband and evidence, fruits, and instrumentalities of violations 18 U.S.C. §§ 2251(a), 2252A(a)(2)(A), and 2252A(a)(5)(B) in the form of the following:

- (a) Records and information constituting child pornography, as defined in 18 U.S.C. 2256(8);
- (b) Records and information constituting child erotica;
- (c) Records and information referencing or revealing sexual activity with or sexual interest in minors or those purporting to be minors;
- (d) Records and information referencing or revealing communications, in any form, of a sexual nature with minors or those purporting to be minors;
- (e) Records or information constituting or revealing the receipt, distribution, or production of child pornography, as defined in 18

U.S.C. 2256(8), or an attempt to commit the same, as well as the identity of any participants;

- (f) Records and information constituting or revealing membership or participation in groups or services that provide or make accessible child pornography;
- (g) Records and information revealing the use and identification of remote computing services such as email accounts or cloud storage;
- (h) Records revealing or indicating the identity of the individual who created and used the account and that individual's location.

As used above, "child erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions. The term "minor" means any person under the age of 18 years.